Browser News - Mozilla

CA/B Forum F2F
October 2023

Ben Wilson

Link to Previous Mozilla May 2023 Face-to-Face briefing - https://cabforum.org/wp-content/uploads/6-2023-May-Mozilla-Update-for-CABF-Redmond-F2F.pdf

Mozilla Root Store Policy (MRSP) v. 2.9 (effective Sept. 1, 2023)

Recent post to the Mozilla Security Blog about MRSP v. 2.9 -
https://blog.mozilla.org/security/2023/09/13/version-2-9-of-the-mozilla-root-store-policy/

CA Communication and Survey -

In the survey, we asked for any questions or concerns about:

- **Reducing root CA lifetimes and the transition schedule**
- **Adoption of the S/MIME BRs and Mozilla's transition guidance**
- **Reporting serious vulnerabilities or security incidents and guidance**
- Audit reporting
- Submission of Compliance Self-Assessments
- Elimination of SHA-1

Survey responses -

We received over 60 responses, including questions/concerns about the first three bullets. Our response is summarized as follows:

MRSP § 7.4 (Root CA Lifecycles) and the Root CA Lifecycles guidance:

Mozilla recommends that CAs not wait until the last moment to request a root CA replacement, but instead ensure sufficient time when both the old and new roots can coexist in the root store.

Provided that the CA has a good compliance history, Mozilla will prioritize with Priority P1 those inclusion requests that involve a root CA replacement - https://wiki.mozilla.org/CA/Prioritization. (For Priority P1, “Applicant has good compliance history and is replacing an already-included CA certificate or is previously approved as a subordinate CA operator”.)

For root CAs enabled with the email trust bit, the “distrust after” mechanism will be used. “Distrust after” will not be used for the websites trust bit. Instead, the websites trust bit will be removed, so CAs will need to cease issuing TLS certificates from deprecated roots at least one year / 398 days prior to the date that the websites trust bit will be removed.

We plan to add a CA Task List Report to the CA Home page in the CCADB to alert CAs well in advance of when they should be working on the replacement for their aging root certificate(s).

S/MIME requirements and Mozilla's transition guidance:

As of September 1, 2023, S/MIME certificates and CA operations must conform to the S/MIME BRs and hopefully CAs have revised their CPs and CPSes to incorporate the S/MIME BRs.

CA operators should modify their CP or CPS on or before September 1, 2023, to assert compliance with the S/MIME BRs. We are not expecting CAs to file an incident report for this.

S/MIME audits should be scoped to include September 2023. An incident report is required if the CA did not begin complying with the S/MIME BRs by 9/1/2023 or if the audit period is not going to include September 1, 2023.

Many CAs are already filing incident reports for S/MIME non-compliance, but we will also be reviewing audit statements as they are submitted.

CAs should file one incident bug covering all ***unreported*** S/MIME non-compliances listed in the audit statement (i.e. all non-compliances arising on or after September 1, 2023).

Those few CAs whose normal audit periods end between September 1, 2023, and October 30, 2023, are expected to submit period-of-time audits that cover their subsequent audit period. For instance, a CA whose normal audit period ends on September 30, 2023, would obtain a period-of-time audit for October 1, 2023, through September 30, 2024, and the audit report would need to be submitted before January 1, 2025.

Vulnerability disclosure and security incident reporting:

MSRP section 2.4 defines incidents, while section 2.4.1 discusses serious vulnerabilities and security incidents. As stated in the Vulnerability Disclosure wiki page, the purpose of section 2.4.1 and the “CA Security Vulnerability” Bugzilla component is to enable CAs to provide Mozilla with “Information about security compromises that require action from Mozilla” and “Security-sensitive information that needs to be shared with Mozilla”.

CAs need to be sure to mark the “CA Program Security” checkbox in such Bugzilla reports.

We welcome suggestions and improvements for the Vulnerability Disclosure wiki page from the CA community, and a discussion thread has been started in MDSP to receive suggestions for updating the wiki page.

CA Inclusion Requests - https://wiki.mozilla.org/CA/Dashboard

Status	Count
Received - Initial Status	13
Information Verification	12
CP/CPS Review Needed	1
Ready for Public Discussion	3
In Public Discussion	1
TOTAL	**30**

CA Compliance - https://wiki.mozilla.org/CA/Incident_Dashboard

Since the beginning of 2023, there have been approximately 95 compliance incidents opened in Bugzilla of the following types. (Current open bugs can be found in the Incident Dashboard.)

Type of Incident	Count
[ov-misissuance] and/or [ev-misissuance]	23
[crl-failure] and/or [ocsp-failure]	17
[disclosure-failure]	12
[smime-misissuance]	7
[dv-misissuance]	6
[leaf-revocation-delay]	6
[audit-finding]	5
[ca-misissuance]	5
[policy-failure]	5
[uncategorized]	5
[ca-revocation-delay]	3
[audit-delay]	1
TOTAL	**95**

Our Email Address: **certificates@mozilla.org**